



Hybrid Threats in the Thai–Cambodian Conflict: A Case Study on Emerging Risks and Cognitive Warfare Readiness

Jeerawat Linakanit¹ & Tatporn Tanawaritt¹

Corresponding Authors: tatporn.tanawaritt@gmail.com

Received:25/03/69 Revised: 30/04/69 Accepted: 01/05/69

Abstract

The escalating prevalence of hybrid threats has fundamentally transformed contemporary conflict, shifting the strategic center of gravity from physical confrontation toward the cognitive domain — where perceptions and belief systems serve as primary targets. The 2025 Thailand–Cambodia conflict provides a critical empirical case, illustrating the multidimensional nature of these threats through coordinated disinformation campaigns and intensified cyber activities integrated with conventional military clashes. This study pursues three objectives: to identify and categorize the hybrid threat instruments employed during the conflict; to evaluate the escalation mechanisms through which hybrid warfare transitions into the cognitive domain; and to propose a strategic framework for national cognitive warfare readiness.

¹ Rajapark Institute



Adopting a qualitative approach, the research employs content analysis of secondary data collected between May and December 2025. Findings indicate that Cambodia's strategy integrated multi-domain non-kinetic operations — encompassing information, psychological, cyber, and influence operations — potentially supported by transnational criminal-state networks, to target cognitive mechanisms. While these activities shaped early international perceptions through narrative competition, they did not reach the full threshold of cognitive warfare due to insufficient long-term strategic integration. Thailand's response, conversely, was characterized by tactical reaction and fragmented communication in the early stages, revealing structural vulnerabilities in addressing sustained cognitive domain influence.

This article contributes to the security literature by introducing a conceptual framework mapping the transition from hybrid warfare to cognitive warfare, identifying the convergence of information environment management and narrative competition — sustained through long-term operational continuity — as the primary drivers of cognitive escalation, ultimately enabling subconscious manipulation and strategic outcomes such as weakened adversary cohesion. To mitigate these risks, the study advances a citizen-centered resilience model integrating robust legal frameworks, Media Information Digital and Algorithm Literacy (MIDAL),



systematic fact-checking, international cooperation, and preemptive strategic communication.

Keywords: Hybrid warfare; Cognitive warfare; Narrative competition; Information operations; Thailand–Cambodia conflict

Introduction

Over the past five years, global geopolitics has undergone a significant transformation, transitioning from unipolarity toward a fragmented multipolar order. This transition has intensified strategic competition among major powers and expanded confrontation across multiple domains, including political ideology, economic influence, technological rivalry, and security. In pursuing geopolitical advantages, major powers increasingly rely on indirect forms of confrontation—such as proxy conflicts and non-kinetic operations—which have introduced complex and diverse threat patterns to the contemporary security environment (Bhardwaj, 2025; Weber, 2025).

Since 2020, many international conflicts have evolved from conventional military confrontations into hybrid warfare. Notable examples include the Russia–Ukraine War, the Gaza conflict, tensions between



Russia and the Baltic states, the Belarus–EU migrant crisis, and cross-strait tensions between China and Taiwan. These cases demonstrate how modern conflicts increasingly integrate military actions with non-military tools designed to manipulate political, social, and informational environments.

Scholars have noted that contemporary warfare is shifting from wars of attrition to "wars of cognition," where the primary battleground extends into the informational and cognitive spheres. In this context, conflict occurs via cyberspace and digital systems, utilizing cyber operations, psychological influence, and soft power to shape perceptions and influence the cognitive processes of political leaders and citizens alike. (Goldfein, 2017; Claverie & Du Cluzel, 2022; NATO Allied Command Transformation, 2024; Backes & Swab, 2019).

In 2025, the Thailand–Cambodia border disputes escalated into an eight-month conflict that caused significant damage. Beyond civilian casualties and mass property destruction, the crisis had profound economic and socio-cultural impacts (Hyma, Thanasin, & Kry, 2026; Rahma, Fitri & Usman, 2026; Chutintaranond & Yurayong, 2026). Historically, Thailand's responses to such operations have been largely reactive—government agencies typically intervene only after disinformation or cyber incidents have occurred, primarily through belated public statements or legal action.



While most existing literature analyzes this conflict through the lens of international relations, this study examines the situation specifically through the framework of cognitive warfare. To address the research question of whether Thailand faces unique strategic challenges in this domain, this article pursues three primary objectives: 1) To identify and categorize hybrid threat instruments employed by Cambodia and Thailand during the conflict. 2) To evaluate the escalation toward the cognitive domain 3) To propose proactive preventive measures aimed at strengthening Thailand's readiness and resilience against emerging cognitive risks.

This study employs a qualitative content analysis of data collected between May and December 2025, including policy reports, media coverage, and digital discourse. While official communications provide the basis for policy analysis, digital discourse—including content from Key Opinion Leaders (KOLs)—is analyzed to capture the dynamics of narrative competition. Finally, the study compares Thailand's experience with international cases, such as the Russia–Ukraine conflict, Ukraine's alliance dynamics, and China–Taiwan tensions to develop preventive measures against emerging risks and enhance Thailand's cognitive warfare readiness.



From Hybrid Warfare to Cognitive Warfare

Over the past decade, the concept of cognitive warfare has received increasing scholarly attention in the study of hybrid conflict. This interest intensified after Annexation of Crimea by the Russian Federation, where Russia combined military pressure with information operations that shaped local perceptions and facilitated political support for annexation. Similar information strategies were later observed in alleged Russian interference in the 2016 United States presidential election and the Brexit referendum. These cases illustrate that information operations can extend beyond influencing opinions to shaping political decisions and social behavior (Bolt, 2021; Llewellyn, et al., 2018).

Cognitive warfare

Cognitive warfare does not merely manipulate information to support military campaigns. Rather, it targets the underlying processes of perception, cognition, and decision-making, aiming to influence behavior at multiple levels—from individuals to entire societies. Cognitive warfare represents an evolutionary shift in strategic competition, moving from the disruption of physical systems to the systematic manipulation of the human mind. The strategic objective extends to broader political, economic, and social domains. By shaping collective perceptions, such operations may



generate long-term strategic advantages, including social fragmentation within adversarial societies and the gradual erosion of trust in institutions (Pastor, 2025; Schmidle, 2026).

Cognitive warfare exploits the interaction between human psychology, information environments, and emerging technologies to persuade, disrupt, or manipulate decision-making processes (Reding & Wells, 2022). These strategies often combine political messaging, psychological operations, information warfare, and cyber-enabled techniques. In the digital era, social media platforms and networked information systems have significantly expanded the operational space for such activities, enabling actors to disseminate narratives rapidly and on a scale. As a result, cognitive warfare increasingly represents a fusion of offensive influence operations and defensive efforts to protect national information environments (Singer & Brooking, 2018).

A central feature of cognitive warfare is the long-term cultivation of influence over cognition. Through sustained exposure to coordinated narratives, target populations may experience a diminished capacity to recognize or respond to emerging threats (Claverie & Du Cluzel, 2022; Backes & Swab, 2019; Karami & Dastenaeei, 2024; Deppe & Schaal, 2024; Gindilā, 2024). Consequently, these populations can become strategic instruments, capable of shaping government policies or constraining the



actions of adversarial states (Tsikhelashvili, 2022; Fenstermacher, et al., 2023, Henschke, 2024).

The efficacy of cognitive warfare is rooted in established psychological vulnerabilities. By weaponizing Cognitive Dissonance, actors deliver information that encourages individuals to rationalize new data in ways that reinforce existing biases. This tendency is reinforced by various Cognitive Bias (Harmon-Jones et al., 2020). Examples include *confirmation bias*, where individuals favor information that supports existing beliefs; *contrast bias*, where relative comparisons make a selected option appear significantly better than alternatives that seem worse; *normality bias*, which leads people to underestimate potential threats; and *status quo bias*, which encourages resistance to change even when alternative options may be more beneficial. Other biases, such as *source amnesia*, where individuals believe misinformation without verifying its origin; *the repetition effect*, where repeated exposure increases perceived credibility even without evidence; and the *backfire effect*, in which individuals confronted with corrective information become more entrenched in their original beliefs.

These psychological vulnerabilities create opportunities for strategic manipulation. A prominent example is Russia's use of the concept of reflexive control, which involves delivering carefully designed information intended to influence an adversary's decision-making process. By shaping



how adversaries interpret available information, actors can guide them toward decisions that ultimately benefit the influencing party while maintaining the illusion of independent choice (Pastor, 2025).

Consequently, the "battlefield" is no longer restricted to physical territory but encompasses the collective consciousness of the target population, where the ultimate strategic outcome is the weakening of national will and social cohesion.

Thailand–Cambodia Conflict Situation

The Thailand–Cambodia conflict escalated on 28 May 2025 following armed clashes in the Chong Bok border area (Cheang & Saksornchai, 2025), rapidly extending beyond the physical battlefield into the digital and informational spheres. On 23 July, Thailand closed all 18 border checkpoints with Cambodia, while the conflict simultaneously expanded online through disinformation and politically sensitive narratives. Information operations were evident in the strategic release and manipulation of content designed to shape public perception and political discourse. (The Better, 2025b).

A notable example occurred on 18 June Cambodian leadership released a recording of a private conversation between Paetongtarn Shinawatra and Hun Sen, triggering significant domestic political fallout (PPTV Online, 2025). The controversy contributed to impeachment



proceedings and ultimately her removal from office by the Constitutional Court on 29 August. (Guzman, 2025).

Diplomatic relations deteriorated further when Thailand downgraded ties with Cambodia on 23 July (Thai PBS, 2025, July 23). Concurrently, cyber activities intensified: Thai authorities reported large-scale distributed denial-of-service (DDoS) attacks targeting government websites, generating over 500 million requests within 24 hours and temporarily disrupting several digital services (Thairath, 2025f)

These developments reflect key characteristics of hybrid warfare, in which military action is integrated with cyber operations, diplomatic pressure, and information manipulation to generate multidimensional strategic effects. Rather than relying solely on conventional force, hybrid strategies exploit vulnerabilities in political institutions, information ecosystems, and public perception. In this context, disinformation campaigns and politically sensitive leaks function as information operations designed to shape narratives and influence political decision-making.

These dynamics also reflect cognitive warfare, which targets the cognitive domain by undermining public perception, political legitimacy, and societal cohesion. By amplifying information controversies and exploiting



political sensitivities, such operations erode institutional trust and deepen internal divisions.

Although Thailand and Cambodia agreed to a temporary ceasefire in Kuala Lumpur on 28 July, tensions resurfaced on 7 December with renewed border clashes. Thailand responded with a military operation dubbed "Century Operation" to counter threats to its sovereignty and reclaim strategic positions. Both countries eventually signed a joint statement on 27 December 2025 declaring a formal ceasefire and cessation of hostilities (Thairath, 2025e).

The Thailand–Cambodia confrontation illustrates how contemporary interstate disputes increasingly extend beyond the battlefield into the informational and cognitive domains, underscoring the growing importance of institutional preparedness and proactive policy responses to hybrid threats.

Hybrid threats against Thailand

The Thailand–Cambodia confrontation illustrates the emergence of multidimensional security challenges commonly described as hybrid threats — coordinated actions by state or non-state actors combining military and non-military instruments to undermine a target state's stability, security, and public confidence (Regan & Sari, 2024; Borch & Heier, 2025). The



evidence shows that hybrid threats operate simultaneously across multiple domains, exploiting political, informational, and societal vulnerabilities through means such as economic coercion, cyberattacks, political interference, and information manipulation. Digital platforms amplify these effects by enabling actors to shape narratives, mobilize public sentiment, and influence decision-making domestically and internationally (Seniutienė & Paulauskytė, 2024). Information-related activities are particularly central to this approach. Disinformation, misinformation, and other forms of information disorder offer low-cost methods for influencing targeted audiences while producing broad strategic effects — and are increasingly deployed alongside conventional military operations.

Several hybrid instruments were deployed alongside kinetic military activities during the confrontation. *Information operations (IO)* involve the coordinated use of information-related capabilities to affect adversary decision-making while protecting one's own, encompassing psychological operations, military deception, and in some doctrines cyber and electronic warfare (Ventre, 2012). *Psychological operations (PSYOP)* exploit cognitive biases through designed narratives and disinformation, using selective framing, exaggerated narratives, and information saturation to shape public attitudes and distort the perceived significance of events (Gergelewicz, 2024; Santos, 2025). *Influence operations* represent a broader strategic approach that integrates soft power, diplomatic, informational, legal, and



economic instruments to shape the perceptions and behaviors of domestic and international audiences across peacetime, crisis, and conflict settings (Claverie & Du Cluzel, 2022; Courter, 2024; Larson et al., 2009). *Cyber operations* — including DDoS attacks, hacking, and phishing — target government systems and digital infrastructure while facilitating disinformation dissemination, with artificial intelligence and algorithmic content distribution further amplifying campaign reach and reinforcing echo chambers (Fenstermacher et al., 2023; Singer & Brooking, 2018; Santos, 2025)

Such activities typically occur within the grey zone, where actions remain below the threshold of conventional warfare yet still pursue strategic objectives through cyber operations, covert influence campaigns, and unmarked forces. Ultimately, hybrid warfare mobilizes military, political, economic, informational, and societal instruments simultaneously to exploit vulnerabilities in an opponent's institutions, economy, social cohesion, and international relationships (Reichborn-Kjennerud & Cullen, 2022).

Hybrid Operational Patterns Employed by Cambodia Against Thailand

Beyond conventional military confrontation, Thailand faced a range of non-kinetic threats prior to the outbreak of armed clashes. In February 2025, Cambodian Ambassador to the United States Koy Kuong signed a lobbying contract with National Consulting Services, Inc. reportedly worth



USD 38,000 per month (The Nation, 2025b) while cyberattacks targeting Thai government websites attributed to Cambodian hacker groups were reported as early as April 2025 (Thairath, 2025a). These developments suggest deliberate efforts to shape the international narrative before military confrontation began. Although direct armed clashes occurred in two phases — 28 May to 28 July and 7 to 31 December 2025 — non-military operations persisted throughout. Activities extended across information operations, cyber operations, and influence operations, illustrating the multidimensional nature of hybrid conflict in which kinetic and non-kinetic instruments are employed simultaneously.

A notable analytical pattern emerging from the conflict is the potential use of proxy-enabled information operations and criminal–state collaboration, in which governments tolerate or indirectly exploit criminal networks to conduct operations while maintaining plausible deniability. Criminal actors serve as intermediaries for cyberattacks, disinformation, and other disruptive activities, enabling states to exert pressure without assuming direct responsibility (Europol, 2025; Rekawek et al., 2025; Tandon, 2023).

The hybrid operational toolkit observed in this conflict can be broadly categorized into four domains: information operations, cyber operations, influence operations, and criminal–state collaboration



Information Operations

Information operations focused on shaping perceptions and controlling narratives combined psychological operations, digital media manipulation, and cyber-enabled dissemination. Disinformation campaigns circulated widely, including false claims that Cambodian houses had been demolished, civilians expelled from contested areas, and cultural sites destroyed (Anti Fake News Center, 2025a), as well as narratives accusing Thailand of ceasefire violations or initiating escalation (Channel 7 News, 2025). Additional campaigns alleged Cambodia ranked among the world's strongest militaries and reported large Thai casualty figures in the Preah Vihear area (Naewna, 2025). AI-manipulated imagery — including staged visuals purporting to show Cambodian forces capturing disputed locations — was widely circulated to bolster domestic morale in Cambodia while undermining confidence among Thai audiences (Anti Fake News Center, 2025b). Further narratives alleged Thai use of chemical weapons, assassination of Cambodian soldiers, and preparation for large-scale invasion, framing Thailand as a powerful state bullying a smaller neighbor to attract international sympathy (Thai Government Spokesman Office, 2025). Information control within Cambodia — through media restrictions



and limited internet access — further constrained the circulation of alternative narratives

Psychological operations appear to have reinforced these efforts through the mobilization of nationalism. Street rallies and protests by Cambodian nationals, led by Hun Many, amplified pro-military sentiment and contributed to significant social media virality. (Ministry of Foreign Affairs, Kingdom of Thailand, 2025b; SE, 2025).

Cyber Operations

Cyber operations constituted another major dimension of the hybrid conflict, encompassing offensive and defensive activities targeting network systems and digital infrastructure. Reported attacks included web defacement, DDoS attacks, and data leaks against Thai institutions (Group IB, 2025). During the peak May–July 2025 period, Thai government and media websites experienced surges in attacks, with one media group reporting up to 200 million attempts in a single day (Post Today, 2025). Hacker groups — including NDTSEC 2.0, NXBBSEC, BL4CK CYB3R, and H3C4KEDZ — publicly announced coordinated campaigns targeting Thai government agencies and private sector organizations under the banner "OptThailand," while AnonSecKh (ANON-KH) threatened attacks against critical infrastructure in education, healthcare, and government services (NT cyfence, 2025; Radware, 2025). Cyber capabilities were also integrated into



broader information operations through coordinated campaigns combining human actors and automated bots to spread disinformation and manipulate social media discourse.

Hun Manet also announced enforcement of a conscription law beginning in 2026 alongside efforts to modernize Cambodia's armed forces, with emphasis on emerging warfare domains including AI and cyber capabilities (Kiripost, 2025).

Influence Operations

A central component involved the mobilization of nationalist narratives by Cambodian political leaders, including Hun Sen and Hun Manet, who promoted hashtags such as #AngkorWat and #ThailandOpenedFire to frame Cambodia as the victim of aggression — simultaneously consolidating domestic support and appealing to international audiences (TNN, 2025). Narrative framing further emphasized allegations of disproportionate Thai force during border air operations and damage to cultural and religious heritage sites, intended to generate international sympathy (Cambodianess, 2025b; Agence France Presse, 2025). The hashtag #DontThaitoMe functioned as an additional framing device, constructing Thailand as dishonest and exploitative (Hyma et al., 2026) while delegitimizing Thai-sourced information as disinformation — contributing to the manipulation of public perception and diffusion of



negative sentiment within the digital sphere. A recurring strategic theme involved portraying Thailand as the primary aggressor through claims of ceasefire violations and threats to Cambodian sovereignty, including allegations of defensive construction near civilian areas. Such framing was intended to invite international intervention or diplomatic pressure on Thailand (Al Jazeera, 2025; Anadolu Agency, 2025; Cambodianess, 2025a).

Influence operations also extended into political and diplomatic arenas. The release of a leaked audio recording involving a conversation between Hun Sen and Paetongtarn Shinawatra reportedly generated political controversy within Thailand, illustrating how information leaks can influence domestic political stability. Additional pressure reportedly included threats to expose Thai politicians such allegations of *lèse-majesté* cases, gambling networks (Bangkok Biz News, 2025b; Thai PBS, 2025b; Thairath, 2025c; Amarin TV, 2026).

Diplomatic and legal instruments were also employed. Cambodia attempted to advance its territorial claims through international legal mechanisms, including efforts to bring disputes before the International Court of Justice (ICJ) based on interpretations of colonial-era maps associated with the Franco–Siamese Treaty (The Diplomat, 2026). Public diplomacy efforts also included hiring international lobbying firms to



influence global media narratives and improve Cambodia's international image (Royal Thai Navy, 2025; Thairath, 2025d). At the same time, Cambodian representatives raised accusations against Thailand in international forums, including allegations of ceasefire violations, the use of chemical weapons and conduct psychological operations in various international forums such as Inter-Parliamentary Union (IPU), United Nations human rights forums (Manager, 2025; The Guardian, 2025).

Economic pressure was another dimension of influence operations. Cambodian authorities announced plans to reduce reliance on Thai electricity and internet infrastructure (The Nation, 2025a) while promoting online campaigns encouraging the boycott of Thai products and tourism, using hashtags such as #BoycottThailand, #BoycottThaiProducts, #BoycottThaiTourism, and #KhmerLoveKhmer (Khmer Times, 2025). Additional measures included travel advisories discouraging international visitors from transiting through Thailand (Kampuchea Thmey Daily, 2025) and calls for Cambodian migrant workers to return home (Bangkok Biz News, 2025a).

Criminal–State Nexus

A further dimension of hybrid conflict concerns collaboration between state actors and transnational criminal networks, enabling states to leverage illicit actors for cyber operations, financial activities, or



information manipulation while maintaining plausible deniability. In this context, allegations have emerged regarding possible links between Cambodian political networks and transnational criminal groups operating call center scams and online fraud networks in areas such as Poipet and Koh Kong, reportedly associated with cybercrime operations targeting Thailand (Money and Banking, 2025).

Some reports also suggest that infrastructure associated with casino zones or special economic areas may have been used as operational hubs supporting cyber activities and information campaigns (The States Times, 2025). Although many of these allegations remain contested, they highlight the growing role of criminal networks as auxiliary actors in hybrid conflict.

The convergence between criminal activity and geopolitical competition represents an emerging dimension of hybrid warfare. By leveraging criminal networks, states may expand their operational toolkit while reducing the risks of direct attribution and escalation.

Thailand's Response to Hybrid Threats

Thailand's response to hybrid threats during the conflict largely took the form of reactive measures across several domains, including information operations, cyber responses, strategic communication, diplomatic action, and economic measures.



Information Operations

Thailand implemented a range of factchecking and counter-disinformation initiatives. Government agencies warned the public about misleading information and encouraged reliance on official communication channels. The Ministry of Foreign Affairs and the Royal Thai Army disseminated daily briefings through social media platforms to provide factual updates and counter narratives emerging from the opposing side (Public Relations Department, 2025b). In parallel, independent fact-checking organizations—including the Anti-Fake News Center, COFACT, ThaiPBS Verify, and MCOT's "Sure Before Share"—worked to verify and debunk misleading information circulating in online spaces.

For Strategic Communication, the government established a Joint Press Briefing Center on the Thailand–Cambodia Border Situation, which issued daily situation reports. Information was disseminated through multiple media channels and in several languages under a “one-message” communication strategy (Sophalkalyan, 2025). These communications emphasized evidence supporting Thailand’s position, including alleged Cambodian violations such as the presence of military equipment in archaeological sites and the seizure of weapons in contested areas. The objective was to present Thailand’s perspective to both domestic audiences and the international community.



Thailand also implemented limited telecommunications controls in response to security concerns. These measures included signal monitoring and the use of jamming technologies after Cambodian reconnaissance drones were detected operating near the border area.

Cyber Operations

Cyber activities formed another dimension of the response. Thai hacker groups and cyber-activist networks such as BlackEye-Thai, CyberSafe TH, and Thai Is God, reportedly conducted retaliatory operations targeting Cambodian digital infrastructure, including systems associated with government agencies, education institutions, and financial services (Group IB, 2025).

Online influence activities employed AI and Bots were also observed. Networks of automated accounts and coordinated messaging campaigns promoted pro-Thailand narratives using hashtags such as #ThailandProtect and #StopCambodiaInvasion (Cambodgemag, 2025). These campaigns sought to mobilize nationalist sentiment and reinforce the legitimacy of Thailand's defensive posture. Coordinated posting patterns (copy-paste) and newly created social media accounts also amplified narratives framing Cambodia as a source of disinformation, particularly involving the hashtag #Scambodia (Thairath, 2025b).

Influence Operations



Thailand employed several influence strategies aimed at shaping public perception. *Narrative management* focused on mobilizing domestic support for national defense and emphasizing themes of sovereignty and security. Campaigns such as “Thailand loves peace but is not afraid to fight” (#ไทยนี้รักสงบแต่ถึงรบไม่ขลาด) were used to reinforce national unity and support for military operations. These efforts have been supported by networks of Key Opinion Leaders (KOLs) (Disa, 2025; ISEAS, (2025).

A parallel component involved challenging the credibility of Cambodian media narratives. Social media campaigns framed Cambodian reporting as misleading or deceptive for example through the hashtag #Scambodia on social media, while promoting alternative narratives highlighting alleged violations of Thai sovereignty, such as #CambodiaOpenFire and #TruthFromThailand. Thailand also sought to shift international public opinion by framing its actions within broader regional security concerns, particularly the suppression of transnational cybercrime networks operating along the border. Within this narrative, Thailand positioned itself as a regional leader in combating scam operations and digital criminal networks (Bloomberg, 2025; Asia Times, 2025; Aljazeera, 2025).

Emotional storytelling was also employed to shape perceptions, including historical narratives portraying Thailand as a long-standing



supporter of Cambodia, such as accounts of humanitarian assistance provided to Cambodian refugees following the collapse of the Khmer Rouge regime, for example the documentary “Camp 511” (One News, 2025).

Official communications repeatedly emphasized principles such as legitimacy, humanitarian principles, transparency, message unity, and morale building—during daily situation briefings to strengthen public confidence and maintain morale.

Legal arguments were presented in international forums to reinforce Thailand’s claim of acting in self-defense. Thai officials accused Cambodia of violating several international legal norms, including attacks on civilian areas, medical facilities (Geneva Convention; Rome Statute), the use of historical sites for military purposes (Hague Convention), and the deployment of anti-personnel landmines (Ottawa Convention) (Public Relations Department, 2025c). These arguments were used to justify Thailand’s response under Article 51 of the United Nations Charter.

Diplomatically, Thailand downgraded relations with Cambodia by recalling its ambassador from Phnom Penh and requesting reciprocal action (Ministry of Foreign Affairs, 2025a). Thai officials also engaged in extensive public diplomacy, providing interviews to major international



media outlets including CNN, BBC, CNA, Al Jazeera, Reuters, and The New York Times (Ministry of Foreign Affairs, 2025 ; Sophalkalyan, 2025; Cambodgemage, 2025). Moreover, Thailand presented Thailand's position in global forums such as the United Nations Security Council (UNSC), the ASEAN Inter-Parliamentary Assembly (AIPA) , the United Nations, the European Union and the Inter-Parliamentary Union (Inter-Parliamentary Union – IPU) (Naewna, 2026; Bangkok Post, 2025; Public Relations Department, 2025a; Daily News, 2025).

Economic pressure was also applied. Thailand closed all 18 border checkpoints and suspended certain internet services in border areas. The government, the Board of Investment (BOI), additionally introduced investment incentives encouraging companies to relocate production facilities from Cambodia back to Thailand.

Cybercrime Suppression

In the field of cybercrime suppression, Thai authorities seized assets worth more than 10 billion baht and issued arrest warrants for several individuals including Kok An, Ly Yong Phat, and Chen Zhi, alleged to be key financiers of cybercrime networks operating in the region (The Better, 2025a; Siamrath, 2025).



Overall, Thailand was able to mobilize a wide range of policy instruments to respond to hybrid threats. However, the response during the early stages of the confrontation was relatively slow compared with the rapid spread of narratives in the digital information environment. This delay allowed early international perceptions of the conflict to form before Thailand's official narrative became widely disseminated. Thailand subsequently reconfigured the narrative landscape, recovering from an initially unfavorable position to gain a more competitive footing in the contest for influence.

Though deliberately response, Thailand's response to the hybrid threats demonstrated a relatively coordinated effort across multiple domains, including cyber defense, diplomatic communication, and law enforcement operations targeting transnational cybercrime networks as demonstrated in Table 1. Authorities implemented fact-checking mechanisms, issued official clarifications, and strengthened cyber defenses to mitigate digital attacks. However, the conflict also revealed structural limitations in countering cognitive and information-based threats.

Table 1: Instruments Employed by Cambodia and Thailand's Countermeasures



Hybrid Threat Domain	Instruments Used by Cambodia	Strategic Objective	Thailand's Response	Limitations of Response
Information Operations	Disinformation campaigns, manipulated images, false casualty reports, chemical weapons accusations	Shape international perception, portray Cambodia as victim	Government fact-checking units, official clarification statements, media briefings	Response slower than disinformation diffusion; limited reach to international audiences
Cyber Operations	DDoS attacks, website defacement, bot amplification, coordinated reporting campaigns	Disrupt information infrastructure and amplify propaganda narratives	Cyber defense operations, blocking malicious traffic, coordination with cybersecurity agencies	Defensive posture only; limited deterrence against external hacker networks
Influence	Nationalist hashtag	Mobilize	Diplomatic	Strategic



Hybrid Threat Domain	Instruments Used by Cambodia	Strategic Objective	Thailand's Response	Limitations of Response
Operations	campaigns (#AngkorWat, #ThailandOpenedFire), diplomatic messaging, lobbying in the United States	domestic support and influence global public opinion	clarification, international communication through MFA channels	communication fragmented across agencies; reactive rather than proactive
Legal and Diplomatic Pressure	Attempts to bring territorial dispute to the ICJ, accusations in international forums	Internationalize the dispute and increase diplomatic pressure on Thailand	Legal preparation, diplomatic protest, bilateral negotiation mechanisms	Legal processes slow; international narrative may form before legal clarification
Economic Pressure	Boycott campaigns against Thai goods and tourism, reduction	Apply economic pressure and	Economic reassurance policies and	Limited ability to counter consumer-



Hybrid Threat Domain	Instruments Used by Cambodia	Strategic Objective	Thailand's Response	Limitations of Response
	of reliance on Thai utilities	mobilize nationalist economic behavior	diplomatic engagement	driven boycott narratives
Criminal– State Nexus	Alleged use of cybercrime networks, call-center scam infrastructure, and gray capital networks	Enable cyber and information operations with plausible deniability	Law enforcement crackdowns and asset seizures related to cybercrime networks	Difficult attribution: transnational criminal networks operate beyond national jurisdiction

While Thailand's responses were institutionally organized, they remained largely reactive, often occurring after disinformation narratives had already spread across digital platforms. In the context of cognitive warfare, the speed of narrative diffusion frequently outpaces state



verification mechanisms, allowing initial misinformation to shape early perceptions among domestic and international audiences. Moreover, fragmented strategic communication across government agencies reduced the effectiveness of coordinated messaging.

As a result, even when factual corrections were later issued, they often struggled to reverse the cognitive impact of earlier disinformation. These dynamics illustrate a broader challenge in contemporary hybrid conflict: states may possess strong defensive capabilities in military and cyber domains yet still face significant difficulties in controlling the information environment and influencing public perception.

Thailand's Domestic Political Fragmentation and Constraints on Strategic Response

Thailand's internal political friction between the government and the military served as a significant bottleneck to its strategic response. Longstanding divisions between conservative elite factions and liberal-leaning blocks created a context of domestic instability that hindered the implementation of state countermeasures. This was evidenced by the leaked phone conversation between Hun Sen and Paetongtarn, in which it was stated that the "Thai military was on the opposing side of Paetongtarn's position" (Strangio, 2025). Although she later framed this as a strategic negotiation tactic (Prachatai, 2025), The incident highlighted



longstanding civil–military antagonisms, particularly given that the Pheu Thai Party—the current successor to earlier Thaksin-aligned parties—emerged from a lineage of parties that were removed from power through military coups in 2006 and 2014, with predecessor parties having been dissolved and reconstituted under new names.

The Constitutional Court's suspension of the prime minister mid-crisis further compounded these vulnerabilities, producing policy discontinuity and weakening state capacity to address external threats. Coalition cohesion collapsed when the Bhumjaithai Party formally withdrew over the government's handling of the crisis (Wongcha-um & Thepgumpanat, 2025). As Bhumjaithai controlled key portfolios — including the Ministries of Interior, Transport, Public Health, and Tourism and Sports — its withdrawal directly impaired Thailand's logistical and administrative capacity. Collectively, this fragmentation of political authority disrupted strategic coherence, undermined a whole-of-government response, and reduced the overall effectiveness of Thailand's ability to counter Cambodia-related threats.

Preparing for the Risk of Cognitive Warfare

The 2025 experience illustrates that contemporary hybrid conflicts extend far beyond conventional military confrontation. Strategic competition increasingly centers on information environments and public perception. In



these contexts, adversaries leverage societal divisions and erode institutional trust, effectively transforming citizens into instruments of strategic influence. These dynamics underscore the ascending importance of cognitive warfare, where the manipulation of public opinion is a primary objective. To mitigate the emerging risks of cognitive war, this study advocates for the development of politically insulated and self-sustaining institutional mechanisms. Such frameworks would diminish the impact of internal political volatility, enabling relevant agencies to operate autonomously while fostering a citizen-centered resilience approach required for long-term national security.

Preparing Thailand to Future Information threats

An examination of hybrid operations during the Thailand–Cambodia tensions suggests that these activities did not reach the threshold of cognitive warfare. The operations failed to significantly alter the perceptions or behaviors of Thai citizens in ways that would advance Cambodia's strategic objectives; in several instances, public awareness of the information operations generated adverse reactions toward Cambodia. Furthermore, the situation did not constitute a comprehensive hybrid threat, as activities lacked full strategic integration across operational domains.

Nevertheless, Cambodia's information operations did influence early international perceptions. Several major international media outlets



initially reported claims suggesting that Thailand had launched the first attack against Cambodia. Although these narratives did not ultimately place Thailand at a military disadvantage, they shaped early global perceptions in ways that temporarily favored Cambodia. The situation also reflects certain characteristics of emerging hybrid threats, particularly through the involvement of non-state actors. Cybercriminal networks and online scam groups were reportedly used as proxies to conduct information operations and undermine public trust in Thai society. However, these activities still lacked a fully coordinated multi-domain strategy.

Although Cambodian information operations have not yet produced significant strategic outcomes, Thailand must prepare for future threats that could affect national security. Preventive measures are necessary to reduce the risk that information operations evolve into more advanced cognitive threats. Notably, even following the December 2025 ceasefire declaration, information operations targeting Thailand reportedly continued into 2026 — including public statements allegedly supporting Pheu Thai Party and People's Party candidates ahead of Thailand's February 2026 elections, Cambodian efforts to secure French expert assistance and legal and technical support for border demarcation disputes, and the circulation of allegations regarding Thai territorial occupation through international media (Reuters, 2026a; Reuters, 2026b).



These developments indicate the need for sustained countermeasures alongside long-term deterrence strategies. Major powers have long conducted operations in the cognitive domain — combining information operations, psychological operations, influence operations, and cyber operations directed at civilian populations — typically sustained over extended periods to gradually shape public perceptions such that target populations make decisions favorable to the initiating actor, often without recognizing external influence. States must therefore strengthen both defensive and proactive responses to hybrid threats to safeguard national sovereignty and protect domestic institutions from external manipulation.

In Thailand's case, this preparedness is particularly pressing given that contemporary conflicts increasingly extend into the cognitive domain. The primary population requiring protection comprises citizens — particularly vulnerable groups such as children, youth, and the elderly, who are disproportionately targeted by information manipulation campaigns. Thailand's preparedness efforts should focus on four key areas: legal frameworks, institutional coordination, technological capacity, and societal resilience.

Preventive measures on emerging risk and counter measures

Legal and Regulatory Frameworks



Thailand currently possesses several legal mechanisms addressing cyber-enabled information threats, including the Cybersecurity Act B.E. 2562, the Computer Crime Act B.E. 2550, the Personal Data Protection Act B.E. 2562, the Digital Government Administration and Service Act B.E. 2562, and the Technology Crime Prevention and Suppression Act B.E. 2566. At the policy level, Thailand has adopted the National Cybersecurity Policy and Action Plan (2022–2027) and introduced cloud cybersecurity standards scheduled to take effect in 2026. Despite this legislative foundation, existing frameworks may prove insufficient should future conflicts escalate into full-scale cognitive warfare (Linakanit & Tanawarit, 2025).

A structural limitation concerns the scope of the National Cyber Security Agency's regulatory authority, which is currently confined to Critical Information Infrastructure (CII) sectors — national security, public services, finance, telecommunications, transportation, energy, and healthcare. Cyber incidents affecting industry, commerce, media and digital infrastructure supporting major national events remain outside comprehensive regulatory oversight, indicating incomplete institutional integration across relevant authorities. Thailand should therefore expand regulatory coverage beyond CII sectors and strengthen coordination among government agencies, the private sector, and international partners. Comparative experience —



notably Ukraine's enhanced cybersecurity collaboration with the European Union and NATO — demonstrates the strategic value of such multilateral cooperation. Strengthening cyber sovereignty over critical digital infrastructure and reducing dependence on foreign technologies should accordingly be treated as a strategic priority.

Media and Information Literacy

Public education aimed at strengthening societal resilience is another essential preventive measure. Developing Media and Information Literacy (MIL) enables citizens to recognize and resist information manipulation.

In Thailand, several institutions promote media literacy. Thai Media Fund supports training programs and curriculum development, while the Public Relations Department and the Office of the National Broadcasting and Telecommunications Commission (NBTC) provide training for citizens, teachers, and youth leaders. Agencies under the Office of the National Digital Economy and Society Commission—such as the Electronic Transactions Development Agency (ETDA), the Digital Government Development Agency (DGA), and the Digital Economy Promotion Agency (DEPA)—also promote Digital Literacy (DL). However, Artificial Intelligence and Algorithm Literacy remain largely unaddressed. This gap is significant because major social media platforms widely used in Thailand such as



Meta, X, TikTok, YouTube, and Line, rely heavily on algorithmic systems that personalize content and may create echo chambers or filter bubbles.

To address this challenge, media literacy initiatives should be integrated into a broader framework combining Media, Information, Digital, and Algorithm Literacy (MIDAL). Such an approach would better equip citizens to understand the technological mechanisms underlying modern information manipulation (Lacourt, 2024; Gindilă, 2024). Special attention should also be given to vulnerable groups, particularly the elderly—who are often targeted by disinformation campaigns.

Fact Checking and Debunking

Thailand currently operates several fact-checking institutions, including the Anti-Fake News Center and Cofact Thailand — established through a collaborative network including ThaiPBS Verify and MCOT's Sure Before Share initiative. However, cooperation with social media platforms remains limited and existing approaches are largely reactive, requiring users to proactively seek verification through official channels.

Comparative models offer instructive alternatives. The European Digital Media Observatory (EDMO) connects fact-checkers, academics, and civil society organizations to monitor disinformation trends and develop coordinated responses, while volunteer networks in the Baltic states — known as 'elves' — assist in countering online propaganda (NATO



StratCom COE, 2022). The European Union has also worked with digital platforms to reduce misinformation spread by adjusting content visibility and removing inappropriate posts (Reuter et al., 2024).

Thailand could strengthen its fact-checking ecosystem by expanding collaboration with digital platforms, improving monitoring systems, and enabling fact-checking organizations to play a more active role in debunking misinformation. The early stages of the Thailand–Cambodia conflict also demonstrated weaknesses in Thailand’s information management. Inconsistent communication from different government agencies generated confusion among the public, highlighting the need for stronger coordination and clearer communication strategies during crises.

Cooperation with Allies

International cooperation represents another important measure for addressing cognitive threats. The European Union has collaborated with digital platforms including Meta, Twitter, and Google through the Code of Practice on Disinformation, which encourages platforms to monitor and remove harmful content — particularly during elections. In 2022, these platforms suspended advertising in Russia and Ukraine to prevent the monetization of disinformation (Ford, 2025). Taiwan has similarly cooperated with social media platforms to identify and address circulating



disinformation, enabling access to AI-based detection systems and real-time content monitoring tools (Hung & Hung, 2022; Zhang, 2020).

For Thailand, expanding international cooperation would strengthen technological capabilities and improve preparedness for emerging cognitive threats by providing access to innovations such as AI-driven detection systems, real-time content monitoring, and collaborative fact-checking frameworks (Institute for Economics & Peace, 2022; Meghraoui & Belkhamza, 2025).

Proactive Communication Measures

Proactive communication plays a crucial role in countering disinformation by disseminating accurate information before false narratives can take hold — creating a 'no-gaps infosphere' in which hostile narratives find little purchase because accurate information has already reached the public, reducing opportunities for fabrication and manipulation (Pripoae-Șerbănescu, 2023; Reuter et al., 2024). A notable example is the prebutter strategy employed by the United States, which rapidly declassified intelligence revealing that Vladimir Putin had already decided to invade Ukraine prior to the outbreak of war, effectively undermining Russia's strategic narrative and strengthening democratic unity (Takagi, 2022).

In Thailand's case, strategic communication should promote a balanced national narrative emphasizing shared interests between the peoples of



both countries, reducing hostility and polarization through multi-perspectival historical interpretation and cultural exchange. Ultimately, effective strategic communication should encourage citizens to move beyond divisive nationalism toward a constructive form of patriotism grounded in civic participation, respect for diversity, and democratic values — strengthening social cohesion while reducing societal vulnerability to external information manipulation. Framing shared civilizational heritage shaped through centuries of regional interaction, rather than narratives glorifying past greatness or constructing adversarial comparisons, offers one such constructive approach.

Summary

The 2025 Thailand–Cambodia conflict exhibits several characteristics of hybrid warfare. Evidence suggests that coordinated non-kinetic activities targeting Thailand had already commenced in early 2025 — prior to the military clash in the Chong Bok area — including information operations, psychological operations, and cyber operations aimed at shaping perceptions and influencing public narratives. Following the outbreak of clashes on 28 May, Cambodia expanded these efforts by integrating military action with information campaigns, psychological operations, cyber operations, and broader influence activities. Observations also indicate potential linkages between state actors and transnational



criminal networks. Thailand responded with countermeasures across multiple domains.

The transition from hybrid to cognitive warfare is illustrated in Figure 1, which presents a conceptual escalation pathway in which non-kinetic activities converge to shape narrative competition within the information environment.

The Thailand–Cambodia case demonstrates how sustained manipulation of the information environment can constitute a trajectory toward formal cognitive warfare.

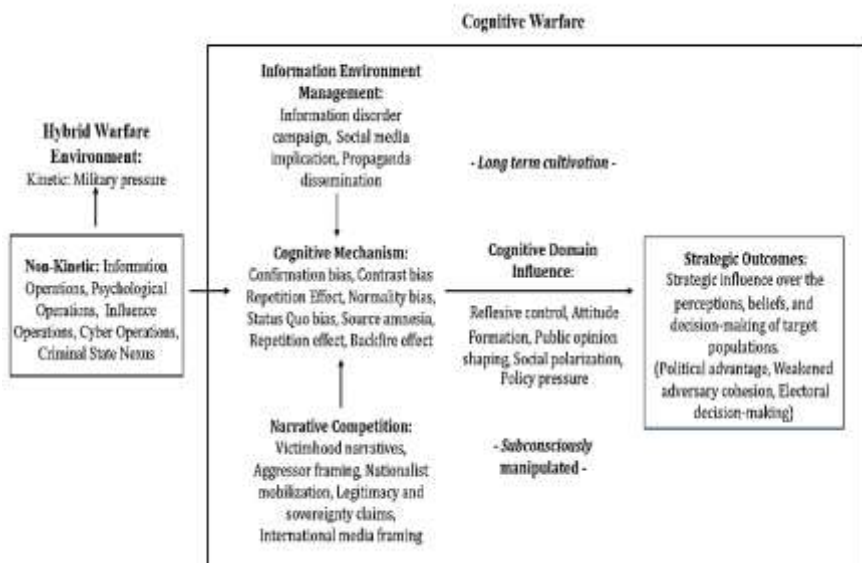


Figure 1: Escalation Pathway from Hybrid Warfare to Cognitive Warfare

Source: Developed by the author



Cambodia's information operations combined disinformation campaigns and civilian information control to manipulate psychological targets. Influence operations sought to secure international support by framing Thailand as the aggressor, leveraging nationalist narratives and international lobbying to enhance Cambodia's global image, while interfering with Thailand's political stability through sensitive information leaks and threats to expose illicit political networks. These efforts were reinforced by diplomatic and legal maneuvers designed to shift the conflict into international legal forums. In the cyber domain, Cambodian operations encompassed web defacement, DDoS attacks, and data leaks targeting Thai institutions.

Thailand's countermeasures operated across several dimensions. Information operations employed reactive measures including factchecking, debunking, and a unified joint communication center. Influence operations encompassed narrative management through a self-defense justification campaign — legitimizing Thailand's military actions within legal and strategic frameworks — and an emotional counter-narrative campaign employing historical storytelling, most notably Thailand's role in sheltering Cambodian refugees, to dismantle the aggressor framing and reposition Thailand as a historically compassionate actor. Legal and public diplomacy engaged major international media and global forums to reinforce the self-



defense narrative. Cyber operations targeted Cambodian digital infrastructure while deploying AI and bot networks to amplify pro-Thailand narratives. However, these countermeasures lacked sustained long-term cultivation: following the formal ceasefire on 27 December 2025, Thai strategic communications were significantly reduced, exposing a structural gap in the long-term investment required for effective cognitive defense.

The Thailand–Cambodia conflict serves as an empirical example of the early stages of cognitive escalation. While initial information operations influenced early international narratives regarding the origin of the clashes, they did not produce a decisive strategic outcome. Nevertheless, they demonstrate how narrative competition can shape perceptions during a crisis's infancy. Although Thailand implemented various countermeasures, most responses remained reactive. Given that contemporary conflicts increasingly extend into the cognitive domain, reactive measures alone may be insufficient. More proactive and long-term strategies are therefore required to prevent the escalation of information operations into sustained cognitive influence campaigns.

This study therefore proposes policy measures to prepare Thailand for potential cognitive warfare risks in the future. The recommendations emphasize citizen-centered resilience to strengthen



society against information manipulation and cognitive threats across five key dimensions.

Legal and regulatory measures. Legal frameworks — particularly the Cybersecurity Act — should be expanded to provide broader protection for critical infrastructure across public and private sectors. Greater institutional integration among relevant agencies and cybersecurity stakeholders would improve early detection of coordinated cyber and information operations.

Media and information literacy. Public resilience should be strengthened through Media and Information Literacy (MIL), particularly among youth and the elderly, evolving toward an integrated Media, Information, Digital, and Algorithm Literacy (MIDAL) framework that equips citizens to understand how digital platforms and algorithms shape information exposure and narrative formation.

Factchecking and debunking. Fact-checking organizations should rapidly verify and debunk misinformation while monitoring abnormal patterns in information flows, disrupting manipulated narratives before they become embedded in public discourse.

International cooperation. Thailand should expand partnerships with international actors and digital platforms to develop systems capable of identifying, flagging, and limiting coordinated disinformation campaigns.



Proactive strategic communication. Strategic communication should proactively shape narratives before hostile actors dominate the information environment, promoting balanced historical understanding, shared cultural heritage, and constructive public discourse that reduces inter-societal hostility.

Regarding limitations, Thailand–Cambodia antagonisms are historically entrenched, whereas this study's data collection was confined to the eight-month period of the 2025 clashes. Future research should examine the long-term cognitive impact of deeply rooted historical conflicts alongside ongoing internal political dynamics. Thailand's political climate — characterized by friction within the governing coalition and between civilian and military leadership — substantially hindered proactive responses, producing a reactive and disunited posture. Future policy development must also account for Thailand's particular political context, as measures strengthening cyber sovereignty inevitably engage tensions surrounding digital rights. Calibrating these measures carefully would enable Thailand to navigate operations more effectively and prevent hybrid threats from escalating into advanced cognitive warfare.



References

- Agence France-Presse. (2025, December 24). *Cambodia slams Thai army for demolishing Hindu statue near border*. Retrieved January 30, 2026, from <https://www.barrons.com/news/cambodia-slams-demolition-of-hindu-statue-by-thai-army-244b4fd9>
- Al Jazeera. (2025, December 11). *Cambodia says Thailand bombed casino hub on border, with no truce in sight*. Retrieved January 30, 2026, from <https://www.aljazeera.com/news/2025/12/18/cambodia-says-thailand-bombs-casino-hub-on-border-with-no-truce-in-sight>
- Amarin TV. (2026, January 12). *Cambodian minister openly supports "Pheu Thai Party" (People's Party of Thailand), points to a way out for Thailand and Cambodia*. Retrieved January 20, 2026, from <https://www.amarintv.com/news/politic/535175/>
- Anadolu Agency. (2025, December 12). *Cambodia urges UN to deploy independent fact-finding mission amid conflict with Thailand*. Retrieved January 20, 2026, from <https://www.aa.com.tr/en/asia-pacific/cambodia-urges-un-to-deploy-independent-fact-finding-mission-amid-conflict-with-thailand/3768998>



Anti Fake News Center. (2025a, December 22). *Beware of fake news!*

Cambodia is accused of using AI to create false information.

Retrieved January 20, 2026, from

<https://www.antifakenewscenter.com/คลังความรู้/ระวังภาพข่าวปลอม-กรณีกัมพูชาใช้-ai-สร้างข้อมูลเท็จ/>

Anti Fake News Center. (2025b, December 26). *Cambodia used AI to*

create false information declaring the seizure of Ta Kwai Temple.

Retrieved January 20, 2026, from

<https://www.antifakenewscenter.com/คลังความรู้/กัมพูชาใช้-ai-สร้างข้อมูลเท็จประกาศยึดปราสาทตาควาย/>

Asia Times. (2025, December 13). *Thais bomb three Cambodian border*

casinos deemed military threats. Retrieved January 30, 2026, from

<https://asiatimes.com/2025/12/thais-bomb-three-cambodian-border-casinos-deemed-military-threats/>

Backes, O., & Swab, A. (2019). *Cognitive warfare: The Russian threat to*

election integrity in the Baltic States. Cambridge, MA: Belfer Center for Science and International Affairs.

Bangkok Biz News. (2025a, June 14). *Hun Sen posted on Facebook urging*

Cambodian workers to return home before being expelled by Thai



authorities. Retrieved January 20, 2026, from

<https://www.bangkokbiznews.com/world/1184877>

Bangkok Biz News. (2025b, August 29). *Urgent! Constitutional Court rules 6:3 to remove Paetongtarn from her position as Prime Minister due to serious ethical violations*. Retrieved January 20, 2026, from <https://www.bangkokbiznews.com/politics/1196381>

Bangkok Post. (2025, September 20). *Cambodia accused of using regional forum to discredit Thailand*. Retrieved January 20, 2026, from <https://www.bangkokpost.com/thailand/general/3107924/cambodia-accused-of-using-regional-forum-to-discredit-thailand>

Bhardwaj, A. (2025). *Geopolitics 2025: The year of great power hedging and contested regional orders*. Retrieved January 10, 2026, from <https://www.faf.ae/home/2025/12/30/geopolitics-2025-the-year-of-great-power-hedging-and-contested-regional-orders>

Bloomberg. (2025, December 18). *Thailand says Cambodia clash is also a war on scammers*. Retrieved January 30, 2026, from <https://www.bloomberg.com/news/articles/2025-12-18/thailand-says-cambodia-border-fight-is-also-a-war-on-scammers>



- Bolt, N. (2021). *Strategic communications and disinformation in the early 21st century* (RSC Policy Paper No. RSC_PP_12). San Domenico di Fiesole, Italy: Robert Schuman Centre for Advanced Studies.
- Borch, O. J., & Heier, T. (2025). *Preparing for hybrid threats to security: Collaborative preparedness and response*. Abingdon, UK: Taylor & Francis.
- Cambodianess. (2025a, December 16). *Cambodia condemns Thai F-16 airstrikes as disproportionate use of force, demands immediate halt*. Retrieved January 30, 2026, from <https://cambodianess.com/article/cambodia-condemns-thai-f-16-airstrikes-as-disproportionate-use-of-force-demands-immediate-halt>
- Cambodianess. (2025b, December 8). *Culture Ministry Condemns Thai Attack, Citing Damage to Conservation Efforts*. Retrieved January 30, 2026, from <https://cambodianess.com/article/culture-ministry-condemns-thai-attack-citing-damage-to-conservation-efforts>
- Cambodgemag. (2025, August 18). *Cambodia & Thailand: The insidious information war in the border conflict*. Retrieved January 30, 2026, from <https://www.cambodgemag.com/en/post/cambodia-thailand-the-insidious-information-war-in-the-border-conflict>



- Channel 7 News. (2025, August 4). *Countering Cambodia's claims, the commander of the 2nd Army Region revealed that Thai soldiers occupied Chong An Ma before the ceasefire agreement*. Retrieved January 20, 2026, from <https://news.ch7.com/detail/818997>
- Cheang, S., & Saksornchai, J. (2025, June 26). *Cambodia ex-leader Hun Sen and Thailand's prime minister make separate visits to tense border areas*. Retrieved January 30, 2026, from <https://apnews.com/article/cambodia-thailand-border-visits-hun-sen-7f2d552cc904f80fc0e88935413dcaf9>
- Chutintaranond, T., & Yurayong, C. (2026). *'Don't Thai to me': A critical discourse and linguistic analysis of border crisis in the Cambodia–Thailand armed conflict*. Retrieved April 27, 2026, from doi:10.1177/17506352261428390
- Claverie, B., & Du Cluzel, F. (2022). "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare. In *Cognitive warfare: The future of cognitive dominance* (pp. 2-1–2-10). Norfolk, VA: NATO Allied Command Transformation.
- Courter, I. J. (2024, August 2). US military doctrine treats information and influence as the same thing—and that's a problem. Retrieved January 8, 2026, from <https://mwi.westpoint.edu/us-military->



doctrine-treats-information-and-influence-as-the-same-thing-and-
thats-a-problem/

Daily News. (2025, November 19). *'Sihesak' prepares to explain the
'Thailand-Cambodia' issue to the international community at a forum
in Belgium*. Retrieved January 10, 2026, from
<https://www.dailynews.co.th/news/5316002/>

Deppe, C., & Schaal, G. S. (2024). *Cognitive warfare: A conceptual analysis
of the NATO ACT cognitive warfare exploratory concept*. *Frontiers
in Big Data*, 7, Article 1452129. Retrieved February 23, 2026, from
[doi:10.3389/fdata.2024.1452129](https://doi.org/10.3389/fdata.2024.1452129)

Disa. (2025, August 10). *Cyber warfare in the Thai-Cambodian border
conflict: The weaponization of information*. Retrieved January 23,
2026, from [https://disa.org/cyber-warfare-in-the-thai-cambodian-
border-conflict-the-weaponization-of-information/](https://disa.org/cyber-warfare-in-the-thai-cambodian-border-conflict-the-weaponization-of-information/)

Europol. (2025). *European Union serious and organised crime threat
assessment: The changing DNA of serious and organised crime
(EU-SOCTA 2025)*. Retrieved January 23, 2026, from
[doi:10.2813/0758057](https://doi.org/10.2813/0758057)



Fenstermacher, L., Uzcha, D., Larson, K., Vitiello, C., & Shellman, S.

(2023). New perspectives on cognitive warfare. In *Signal processing, sensor/information fusion, and target recognition XXXII*

(Vol. 12547, pp. 172–187). Bellingham, WA: SPIE.

doi:10.1117/12.2666777

Ford, A. (2025). *Disinformation and cognitive warfare*. Retrieved January 10, 2026, from

<https://static1.squarespace.com/static/5b7ea2794cde7a79e7c00582/t/67cf0e1db064512e327bdaa1/1741622813495/apo-nid329632.pdf>

Gergelewicz, T. (2024). *Countering disinformation concept for building social resilience in times of cognitive warfare*. Retrieved January 8, 2026, from doi:10.37055/pno/200300

Gîndilă, F. M. (2024). *Manipulating perceptions and behavior through cognitive warfare in the digital age*. In Proceedings of the International Scientific Conference Strategies XXI (pp. 73–78). Bucharest, Romania: Carol I National Defence University Publishing House.

Goldfein, D. L. (2017). *2017 Air, space, and cyber symposium*. Retrieved February 23, 2026, from



http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf

Group IB. (2025, July–August). *Hactivist at war: The Cambodia-Thailand cyber escalation July–August 2025*. Retrieved January 20, 2026, from <https://www.group-ib.com/resources/research-hub/hactivist-at-war-july-august-2025/>

Guzman, C. (2025, August 29). *Thai court removes prime minister—again*. Retrieved January 30, 2026, from <https://time.com/7313316/thailand-paetongtarn-shinawatra-prime-minister-removed-constitutional-court-verdict-pheu-thai/>

Harmon-Jones, E., Harmon-Jones, C., & Levy, N. (2020). *Novel modes of dissonance reduction: Justification of support for Donald Trump*. Retrieved January 30, 2026, from https://www.researchgate.net/publication/346008129_Novel_Modes_of_Dissonance_Reduction_Justification_of_Support_for_Donald_Trump

Henschke, A. (2024). *Cognitive warfare: Grey matters in contemporary political conflict*. New York: Routledge.



Hung, T., & Hung, T. (2022). *How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars*. Retrieved January 30, 2026, from doi:10.1093/jogss/ogac016

Hyma, R., Thanasin, P., & Kry, S. (2026). *New trenches of battle: Cambodian–Thai culture clashes in the digital age of nationalism*. Retrieved February 23, 2026, from doi:10.1177/17506352251415291

Institute for Economics & Peace. (2022). *The Ukraine Russia crisis: Terrorism briefing. The unfolding cyberwar in Ukraine* (IEP Briefing Series 4). Sydney, Australia: Author.

ISEAS. (2025, November 3). *Digital influence and controversies: The role of KOLs and social media in the Thailand-Cambodia dispute* (ISEAS Perspective 2025/82). Singapore: ISEAS–Yusof Ishak Institute.

Khmer Times. (2025, November 26). *Economist exhorts global community to stop buying Thai products*. Retrieved January 30, 2026, from <https://www.khmertimeskh.com/501796102/economist-exhorts-global-community-to-stop-buying-thai-products>

Kampuchea Thmey Daily. (2025, August 18). *Avoid Bangkok, Fly Direct: Cambodia Urges Safer Routes as Transit Risks Mount*. Retrieved



January 30, 2026, from <https://www.kampuchearthmey.com/kpt-english/1039806?>

Karami, A., & Dastenaeei, A. M. (2024). *The European Union's approach to cognitive warfare's command and control*. Retrieved February 23, 2026, from doi:10.52783/jes.7939

Kiripost. (2025, December 17). *Call For Military to be Equipped with Modern Warfare Skills As Military Draft Looms*. Retrieved January 20, 2026, from <https://kiripost.com/stories/call-for-military-to-be-equipped-with-modern-warfare-skills-as-military-draft-looms>

Lacourt, A. (2024). *Media literacy and the empowerment of users*. Retrieved January 22, 2026, from <https://www.obs.coe.int/en/web/observatoire/-/new-report-media-literacy-and-the-empowerment-of-users>

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., & Thurston, C. Q. (2009). *Foundations of effective influence operations: A framework for enhancing army capabilities*. Retrieved January 18, 2026, from <https://apps.dtic.mil/sti/pdfs/ADA503375.pdf>



Linakanit, J., & Tanawarit, T. (2025). Enhancing cybersecurity capacity: Thailand's challenges and responses in the context of hybrid warfare. *Arts of Management Journal*, 9(4), 1–23.

Llewellyn, C., Cram, L., Favero, A., & Hill, R. L. (2018). Russian troll hunting in a Brexit Twitter archive. In *Proceedings of the 18th ACM/IEEE on Joint Conference on Digital Libraries* (pp. 361–362). New York: ACM.

Manager. (2025, July 30). *Cambodia is twisting the truth again! They accused Thailand in the Inter-Parliamentary Union of violating the ceasefire and using chemical weapons, injuring Cambodians. "Van Nor" retaliated with condemnation and a statement to the world.* Retrieved January 20, 2026, from <https://mgronline.com/politics/detail/9680000071947>

Meghraoui, L., & Belkhamza, Z. (2025). *Cognitive warfare and cybersecurity: Strategic implications for global security*. In Proceedings of the 19th International Conference on Cyber Warfare and Security. Reading, UK: Academic Conferences and Publishing International.

Ministry of Foreign Affairs, Kingdom of Thailand. (2025a, July 24). *Statement on Thailand-Cambodia situation*. Retrieved January 20,



2026, from <https://www.mfa.go.th/en/content/statement-on-th-cam-situ-24-jul-25-eng>

Ministry of Foreign Affairs, Kingdom of Thailand. (2025b, September 17).

Statement on the incursion and protest by Cambodian nationals in Ban Nong Ya Kaew, Khok Sung district, Sa Kaeo province.

Retrieved January 20, 2026, from

<https://mfa.go.th/en/content/statement-091725-en?cate=5d5bcb4e15e39c306000683e>

Ministry of Foreign Affairs, Kingdom of Thailand. (2025c, December 10).

Summary of the press briefing on the developments of the Thailand–Cambodia border situation on 10 December 2025.

Retrieved January 20, 2026, from

<https://www.mfa.go.th/en/content/press-briefing-10dec25>

Money and Banking. (2025, July 28). Cambodian call center gangs have turned to information operations (IO) warfare, attacking Thailand with over 500 million attacks per day. *Money and Banking.*

Retrieved January 10, 2026, from

<https://moneyandbanking.co.th/2025/187048/>

Naewna. (2026, July 26). The Thai representative's statement to the UNSC reads: "Thailand is committed to peace, but Cambodia attacks



indiscriminately. We must defend ourselves.". Retrieved January 10, 2026, from <https://www.naewna.com/politic/902231>

Naewna. (2025, October 21). Cambodians are deceiving themselves!

They're using information operations (IO) to spread misinformation, claiming the Cambodian army is ranked 6th strongest in the world.

Naewna. Retrieved January 10, 2026, from <https://www.naewna.com/likesara/922627>

NATO Allied Command Transformation. (2024, July 3). *Allied Command Transformation develops the cognitive warfare concept to combat disinformation and defend against "cognitive warfare."* Retrieved January 8, 2026, from <https://www.act.nato.int/article/cogwar-concept/>

NATO Strategic Communications Centre of Excellence. (2022). *Baltic elves: Citizen-driven responses to Russian disinformation.* Retrieved January 8, 2026, from <https://stratcomcoe.org/publications/download/RUS-Info-Influence-Operations-in-Nordic-Baltic-DIGITAL-V2.pdf>

NT cyfence. (2025, June 11). *Surup hetkan kan chomti thang saiber chak khaempein "OptThailand" [Summary of cyberattack incidents from the "OptThailand" campaign] [Thai-language article].* Retrieved



January 20, 2026, from <https://www.cyfence.com/article/attack-optthailand-2025/>

One News. (2025, October 13). *Documentary about the 511 Cambodian refugees fleeing for their lives at the camp premieres* [Video].

Retrieved January 20, 2026, from

<https://www.youtube.com/watch?v=EhT9J-cC2BI>

Pastor, A. (2025). *Cognitive warfare: The weaponisation of the science of brain and behaviour*. Retrieved January 8, 2026, from

<https://hal.science/hal-04420986v2>

PPTV Online. (2025, June 18). *Hun Sen admits to having a full 17-minute audio clip of his conversation with Prime Minister Yingluck*

Shinawatra, with 9 minutes leaked. Retrieved January 10, 2026,

from <https://www.pptvhd36.com/news/ต่างประเทศ/250931>

Prachathai. (2025, July 11). *Thai military overreach in the Thai-Cambodian conflict: a chronology*. Retrieved January 10, 2026, from

<https://prachataienglish.com/node/11464>

Priopae-Serbănescu, C. (2023). Cognitive warfare – Beyond dominance, manoeuvres and information – The battle for the imagined future.

Romanian Military Thinking, 2023(4), 258–279.



Post Today. (2025, July 27). *Cambodia's IO cyberattacks target Nation Group media over 200 million times*. Retrieved January 10, 2026, from <https://www.posttoday.com/general-news/727843>

Public Relations Department. (2025a, November 24). *Inspection report of the ASEAN Observer Team–Thailand on recent landmine incident* [Press release]. Bangkok, Thailand: Government Public Relations Department, Kingdom of Thailand.

Public Relations Department. (2025b, September 28). *Foreign Minister Sihasak Phuanketkeow speaks about Thai-Cambodian border situation*. Bangkok, Thailand: Government Public Relations Department, Ministry of Foreign Affairs of Thailand.

Public Relations Department. (2025c, July 27). *Summary of press briefing on the Thailand-Cambodia border situation on 27 July 2025*. Bangkok, Thailand: Government Public Relations Department, Ministry of Foreign Affairs of Thailand.

Radware. (2026, June 16). *Cyber Escalation in Southeast Asia: AnonSecKh Targets Thailand*. Retrieved January 10, 2026, from <https://www.radware.com/security/threat-advisories-and-attack-reports/cyber-escalation-in-southeast-asia-anonseckh-targets-thailand>



- Rahma, A. A. N., Fitri, S., & Usman, F. A. (2026). Inclusive Governance Under Fire: Assessing the Breakdown of Border Management Between Thailand and Cambodia in 2023-2025. *PROIROFONIC*, 1(1), 109-117.
- Reding, D. F., & Wells, B. (2022). Cognitive warfare: NATO, COVID-19 and the impact of emerging and disruptive technologies. In R. Gill & R. Goolsby (Eds.), *COVID-19 disinformation: A multi-national, whole of society perspective*. New York: Springer.
- Regan, M., & Sari, A. (Eds.). (2024). *Hybrid threats and grey zone conflict: The challenge to liberal democracies*. Oxford, UK: Oxford University Press.
- Reichborn-Kjennerud, E., & Cullen, P. (2022). *What is hybrid warfare?* Oslo, Norway: Norwegian Institute for International Affairs (NUPI).
- Rekawek, K., Lanchès, J., & Zotova, M. (2025, September). *Russia's crime-terror nexus: Criminality as a tool of hybrid warfare in Europe*. Retrieved January 10, 2026, from <https://icct.nl/publication/russias-crime-terror-nexus-criminality-tool-hybrid-warfare>
- Reuter, C., Lee Hughes, A., & Buntain, C. (2024). Combating information warfare: State and trends in user-centred countermeasures against



fake news and misinformation. *Behaviour & Information Technology*, 44(1), 1–14.

Reuters. (2026a, February 5). *Cambodia asks France to provide historical evidence to help settle Thai border dispute*. Retrieved February 23, 2026, from <https://www.reuters.com/world/asia-pacific/cambodian-pm-says-thailand-occupying-territory-after-trump-brokered-ceasefire-2026-02-18/>

Reuters. (2026b, February 18). *Exclusive: Cambodian PM says Thailand is occupying territory after Trump-brokered ceasefire*. Retrieved February 23, 2026, from <https://www.reuters.com/world/asia-pacific/cambodian-pm-says-thailand-occupying-territory-after-trump-brokered-ceasefire-2026-02-18/>

Royal Thai Navy. (2025, December 16). *In short! Cambodia has hired US lobbyists* [Facebook post]. Retrieved January 10, 2026, from <https://www.facebook.com/RoyalThaiNavyFanpage/posts/สรุปจบที่เตี๋ยว-กัมพูชาจ้างล็อบบียิสต์สหรัฐเอ็กซารว่อนเน็ตคือของจริงหรือแค่ข่าวล/1347308897431423/>

Santos, C. P. (2025). Cognitive warfare: The mind as a battlefield. *Eksplorium: Buletin Pusat Teknologi Bahan Galian Nuklir*, 46(1), 1243–1270.



- Schmidle, R. (2026). Understanding cognitive warfare: Beyond information. *PRISM*, 11(2), 46–63.
- SE, S. (2025, June 18). *Cambodian government musters support from huge crowds in Thai border row*. Retrieved January 30, 2026, from <https://www.japantimes.co.jp/news/2025/06/18/asia-pacific/politics/cambodia-support-thai-border/>
- Seniutienė, D., & Paulauskytė, L. (2024). Response to hybrid threats: Policies, concepts and strategic approaches. *Public Security and Public Order*, 36, 195–202.
- Siamrath. (2025, November 9). *Arrest warrants have been issued for Lee Yong-phat and five others on charges of conspiracy and money laundering, following strong evidence linking them to a scammer operation after cyber police and the Anti-Money Laundering Office (AMLO) conducted searches at 36 locations*. Retrieved January 10, 2026, from <https://siamrath.co.th/quality-of-life/crime/109220>
- Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Boston: Eamon Dolan Books.
- Sophalkalyan, J. (2025, August 9). *Why Cambodia is losing the information war with Thailand*. Retrieved January 30, 2026, from



<https://thediplomat.com/2025/08/why-cambodia-is-losing-the-information-war-with-thailand/>

Strangio, S. (2026, June 3). *Cambodia Says It Will Take Thai Border Dispute to International Court*. Retrieved January 20, 2026, from <https://thediplomat.com/2025/06/cambodia-says-it-will-take-thai-border-dispute-to-international-court/>

Strangio, S. (2025, June 19). *Thai government rocked by withdrawal of major coalition party*. Retrieved January 30, 2026, from <https://thediplomat.com/2025/06/thai-government-rocked-by-withdrawal-of-major-coalition-party/>

Takagi, K. (2022, July 22). *The future of China's cognitive warfare: Lessons from the war in Ukraine*. Retrieved January 20, 2026, from <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>

Tandon, B. (2023). State crime: Exploring the nexus between power, politics and organized criminal networks. *Law & Political Review*, 8, 192–204.

Thai Government Spokesman Office. (2025, August 1). *Responding to Cambodia's 4 false accusations* [Facebook post]. Retrieved



January 20, 2026, from

<https://www.facebook.com/ThaigovSpokesman/posts/1180846584078071/>

Thai PBS. (2025a, June 27). *Hun Sen threatens to expose Thaksin for lese majeste*. Retrieved January 20, 2026, from

<https://www.thaipbs.or.th/news/content/353651>

Thai PBS. (2025b, July 23). *Bhumtham orders strong reinstatement of Thai ambassador and expulsion of Cambodian ambassador over Chong Anma bombing*. Retrieved January 10, 2026, from

<https://www.thaipbs.or.th/news/content/354575>

Thairath. (2025a, June 10). *Arrest warrants issued for Cambodian hackers accused of attacking Thai government websites in retaliation for the ongoing Thai-Cambodian border situation*. Retrieved January 20, 2026, from <https://www.thairath.co.th/news/local/2863615>

Thairath. (2025b, December 24). *Cambodia Warns Citizens to Stop Sharing Distorted Content from Thailand*. Retrieved January 20, 2026, from <https://en.thairath.co.th/news/foreign/2903821>

Thairath. (2025c, October 15). *Hun Sen issues a strong warning! Threatens to crack down on gambling websites targeting Thai politicians if*



border crossings are not reopened. Retrieved January 20, 2026, from
https://www.thairath.co.th/video/channel/thairath_news/thairath-news-show/1169995

Thairath. (2025d, December 17). *Meet the top US lobbyists who are helping gain a strategic advantage through communication.* Retrieved January 20, 2026, from
<https://www.thairath.co.th/scoop/theissue/2902564>

Thairath, 2025e, December 10). *The Royal Thai Army announces, "Operation Century," honoring the brave soldiers who sacrificed their lives to protect Thailand.* Retrieved January 20, 2026, from
<https://www.thairath.co.th/news/local/2901012>

Thairath. (2025f, July 28). *24-hour monitoring: Cambodian hackers launch over 500 million DDoS attacks.* Retrieved January 20, 2026, from
<https://www.thairath.co.th/lifestyle/tech/2873293>

The Better. (2025a, July 8). *An arrest warrant has been issued for "Kok An," a close associate of "Hun Sen," in connection with a call center scam. Cyber police raided 19 locations across three provinces. The* Retrieved January 30, 2026, from
<https://www.thebetter.co.th/news/news/32364>



The Better. (2025b, July 23). *"Bhumtham" orders recall of Thai ambassador and downgrades relations with Cambodia after Thai soldier's leg is amputated by landmine*. Retrieved January 30, 2026, from <https://www.thebetter.co.th/news/news/33099>

The Guardian. (2025, October 17). *'Wailing ghosts through loudspeakers': Cambodia accuses Thailand of psychological warfare along border*. Retrieved January 30, 2026, from <https://www.theguardian.com/world/2025/oct/17/cambodia-accuses-thailand-psychological-warfare-border>

The Nation. (2025a, June 13). *Cambodia to stop importing electricity and internet from Thailand*. Retrieved January 20, 2026, from <https://www.nationthailand.com/news/general/40051184>

The Nation. (2025b, December 16). *"Don Benton", a "Trump ally" lobbying for "US backing for Cambodia"*. Retrieved January 20, 2026, from <https://www.nationthailand.com/news/general/40059862>

The Nation. (2025c, July 27). *Nation Group hit by 200 million cyberattacks in Cambodian IO campaign*. Retrieved January 20, 2026, from <https://www.nationthailand.com/blogs/news/asean/40053189>



- The States Times. (2025, September 15). *The BBC has faced heavy criticism after releasing the documentary "The Dark Side of Thailand," raising suspicions of distortion, devaluation of Thailand, and links to illicit businesses in Cambodia*. Retrieved January 30, 2026, from <https://thestatestimes.com/post/2025091503>
- TNN. (2025, August 2). *"Information Operation" by Cambodia attacks Thai social media* [Video]. Retrieved January 20, 2026, from <https://www.youtube.com/watch?v=7mtMulVApOw>
- Tsikhelashvili, N. (2022, May 6). Influence of cognitive warfare on national will to fight. Retrieved January 8, 2026, from <https://www.thedefencehorizon.org/post/influence-of-cognitive-warfare-on-national-will-to-fight>
- Ventre, D. (2012). *Information warfare*. Hoboken, NJ: John Wiley & Sons.
- Weber, N. A. (2025, June 25). *Technology, apathy, and proximity: The holy trinity of hybrid warfare*. Retrieved January 8, 2026, from <https://www.geopoliticalmonitor.com/technology-apathy-and-proximity-the-holy-trinity-of-hybrid-warfare/>



Wongcha-um, P. & Thepgumpanat, P. (2025, June 18). *Bhumjaithai party exits Thailand's coalition government*. Retrieved January 20, 2026, from <https://www.reuters.com/world/asia-pacific/bhumjaithai-party-exits-thailands-coalition-government-2025-06-18/>

Zhang, L. (2020). *How to counter China's disinformation campaign in Taiwan*. Retrieved January 8, 2026, from <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-20/Zhang-Disinformation-Campaign-1.pdf>